Raytheon

Security for Real-Time Military Systems

Open Systems Project Engineering Conference (OSPEC)

FY 98 Status Review

29 April - 1 May 1998

Bill Smith

Defense Information Systems Agency

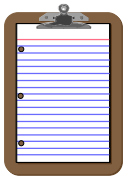
(smith2b@ncr.disa.mil)

Dale Wolfe

Raytheon Systems Company

(dgwolfe@mail.hac.com)

Project Number 40 Overview
Agenda



- Participants and Standards Bodies
- Purpose and Goals
- FY97 Tasks
- Background and Objective of the “Delta Document Security Addendum”
- What Are the Threats Out There
- Partitioning the Security Requirements
- A Look at the Requirements
- “Delta Document Security Addendum” Summary
- FY98 Summary

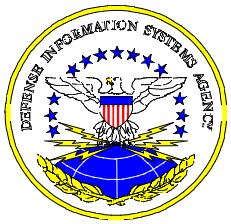
Raytheon

Participants and Standards Bodies

- **Key Participants:**
  - **DISA / JIEO CFS**
  - **SPAWARSYSCEN San Diego (formerly NRaD)**
  - **Lloyd LaMont Design**
  - **Raytheon Systems Company (formerly Hughes Electronics)**
- **Standards Bodies:**
  - **IEEE Portable Application Standards Committee (PASC)**
  - **The Open Group**
  - **Object Management Group (OMG)**
  - **W3C (WWW Consortium)**

Raytheon

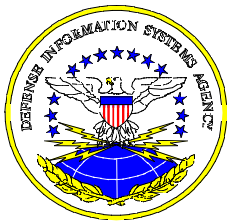
Purpose



- **Fill the Existing Void for Advanced Systems.**
- **Define a Standard Interface and Environment for Computer Operating Systems that require:**
  - **(1) Security Mechanisms and/or**
  - **(2) A Secure Environment**
- **Define a Framework for Security within Distributed Open Systems.**
- **Identify the Required Security Service Primitives of the Framework.**

Raytheon

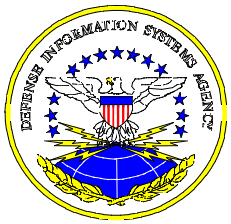
Goals



- **Keep the Industry Momentum Going, Govt Participation.**
- **Support, Advance and Complete the Development of POSIX Security Drafts:**
  - **P1003.1e -- Protection, Audit and Control Interfaces. (Sited in v2 of the JTA)**
  - **P1003.2c -- Protection and Control Utilities.**
  - **P1003.22 -- Security Framework / Guide for POSIX Open System Environment. (Sited in Version 2 of the JTA) [The Open Group]**
- **Foster Acceptance of Real-Time Security Requirements Within The DoD and Standards Communities:**
  - **IEEE PASC, The Open Group**
  - **International Organization of Standardization (ISO)**
  - **Major DoD Organizations, Offices and Programs.**

Raytheon

FY97 Tasks



- **Survey the Draft POSIX Security Standards, and Real-Time Weapon Systems / Avionics Systems Security Requirements.**
- **Identify Security Services not Present in POSIX, but Critical to Military and Industrial Real-Time Partmers.**
- **Generate a "Delta Document Security Addendum" for Embedded Real-Time Military Systems.**
- **Promote Real-Time Embedded Security Within IEEE PASC:**
  - **Participate in Current Security Working Group Activities.**
  - **Pursue the Creation of a POSIX Study Group to Address System Security Issues.**

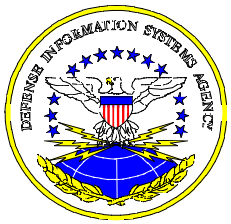
Raytheon

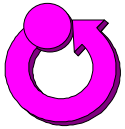
Background on the "Delta Document Security Addendum"

- Delta Document was completed and Delivered in October 1996.
- A Statement of Work for Delta Document follow-on work was submitted in January 1997.
- The Security Task was funded in May 1997 to:
  - Evaluate security features of real-time military systems.
  - Evaluate the security features of POSIX.
  - Provide an Addendum to the Delta Document with the security findings.
  - Develop an action plan to present the findings to the pertinent working groups.
- The "Delta Document Security Addendum" was delivered to NRAD in September 1997.

Raytheon

The Objective of the "Delta Document Security Addendum"

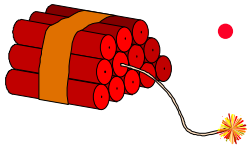




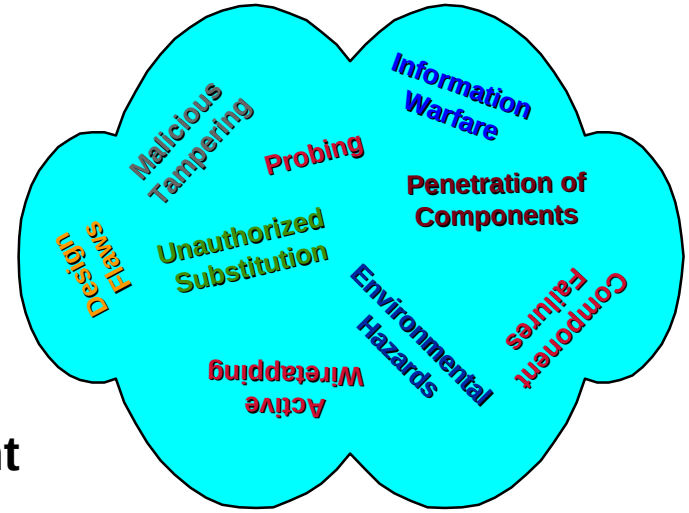
- Address Security Requirements for Real-Time Military Operating Systems.
- Discuss Threats to Avionics Systems encountered at all Phases of the Avionics Component's life.
- Discuss Typical Security Models.
- Assess the functionality defined by POSIX to the requirements described in the addendum document.
- Assess the functionality of the Hughes AOS to the requirements described in the addendum document.
- Document an OS Level Functional Comparison of the above Assessments.

Raytheon

What Are The Threats Out There



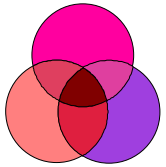
- A Threat is ... *Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification or data, and/or denial of service*
- Threats to Military Avionics
  - Common Threats
  - During Field Test
  - From The Training Environment
  - From The Operations Environment
  - From the Maintenance Environment



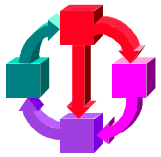
- Attacks
- Threats to Real-Time Embedded Systems

Raytheon

Partitioning the Security Requirements



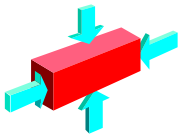
- **Abstractions:**
  - **Operating System Level ...contains all of the primitive services and functionality used to support security access and enforcement**
  - **Policy Level ... addresses the rules used to enforce security.**
  - **Enforcement Level ... contains the high level mechanisms that apply the security policy.**



- **Configurations:**
  - **Centralized Security Levels.**
  - **Distributed Security Levels.**
  - **Dual Application Program Interfaces (APIs).**

Raytheon

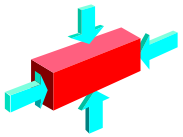
Let us Look at the Requirements



- **Operating-System-Level Requirements.**
  - **Low-Level Functionality.**
  - **Control Address Space.**
  - **Restrict System Object Access.**
  - **Support Time-Critical and Non Time-Critical Services.**
  - **Limit the Dynamic Allocation of Resources by a Subject.**
  - **Support Mechanisms to Unambiguously pair Security Labels to a Subject or an Object.**

Raytheon

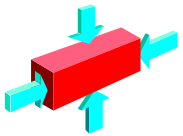
Let us Look at the Requirements



- **Policy-Level Requirements.**
  - **Define the Security Rules for all Modes and Configurations of the System.**
  - **Define Security Rules for Objects that may be Imported or Exported.**
  - **Define Rules Restricting Subject accesses of Objects based on Sensitivity, Compartment, and Access Mode.**
  - **Define Access Modes.**
  - **Define Sensitivity Levels.**
  - **Define Compartment Levels.**

Raytheon

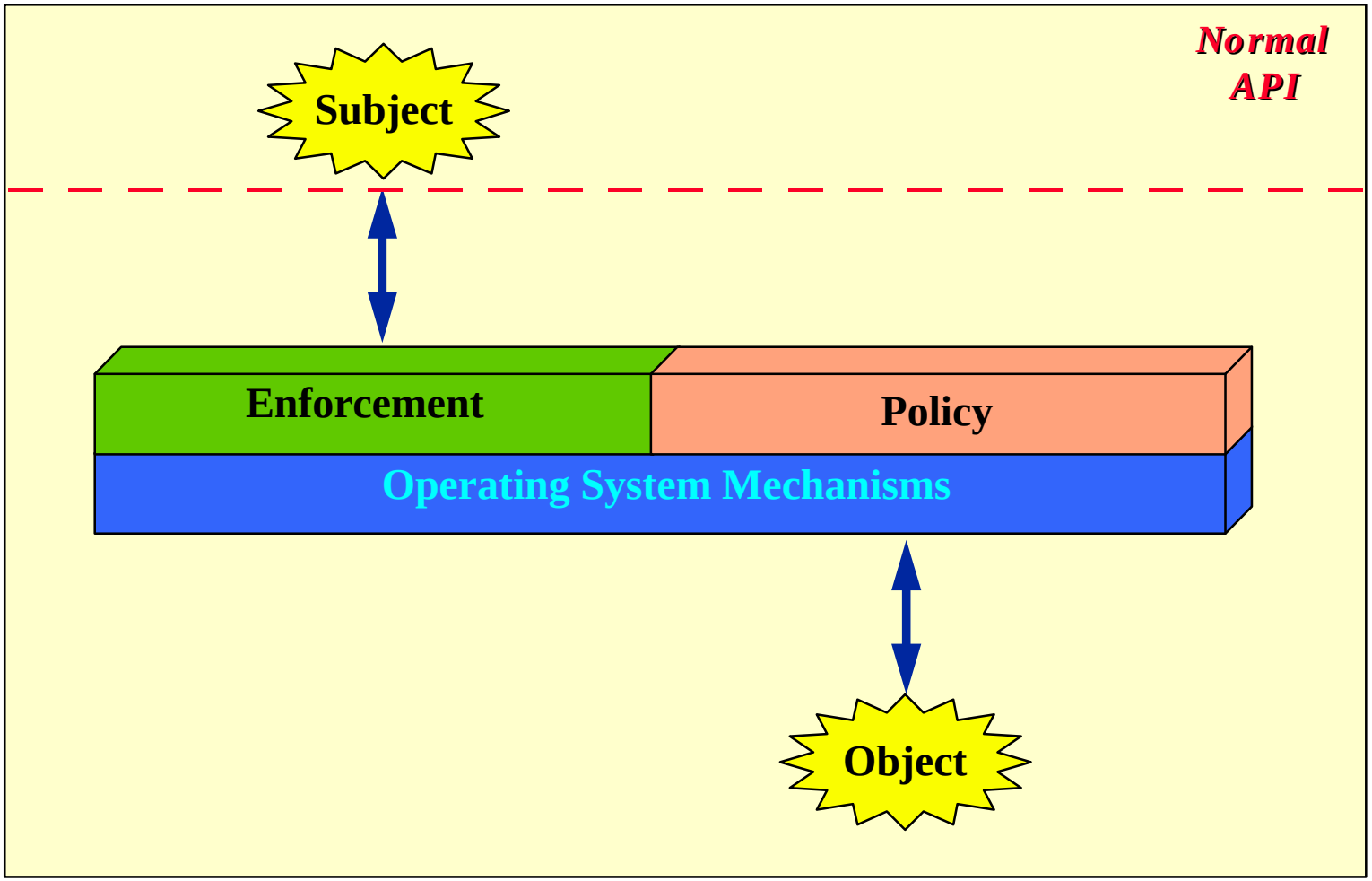
Let us Look at the Requirements



- **Enforcement-Level Requirements.**
  - **Provide and Protect Audit Logs.**
  - **Log Transactions.**
  - **Assign System-Wide Security Labels.**
  - **Protect Security Labels.**
  - **Restrict the change of Security Levels to Owners of the Objects.**
  - **Deny any Requests that Violate the Security Policy.**
  - **Bind All Subject Requests to Objects.**
  - **Authenticate and Verify Subject Requests using the Security Policy.**
  - **Detect and Log Violations.**
  - **Deactivate an Offending Subject to prevent further Violations.**

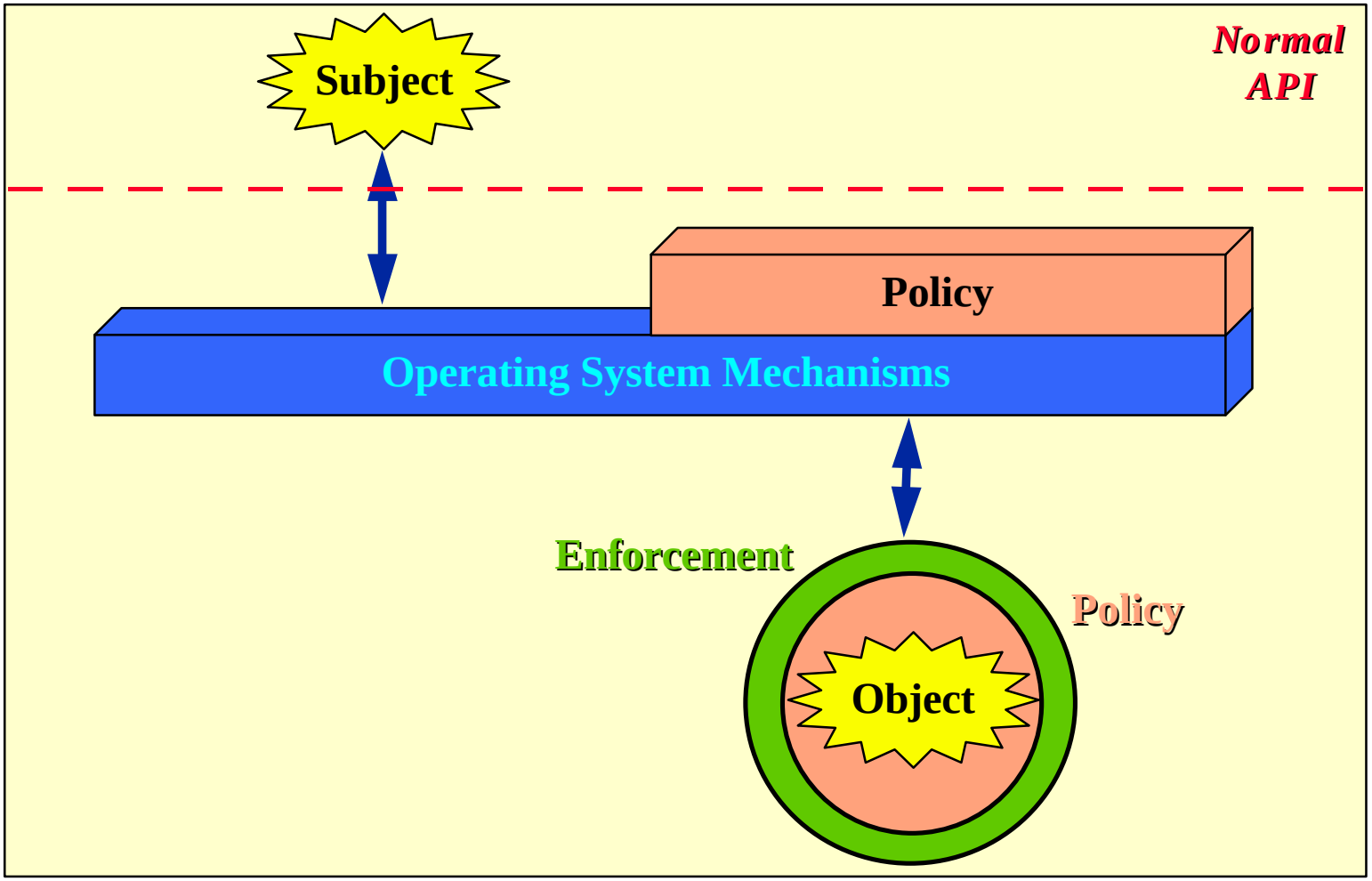
Raytheon

Centralized Security Levels



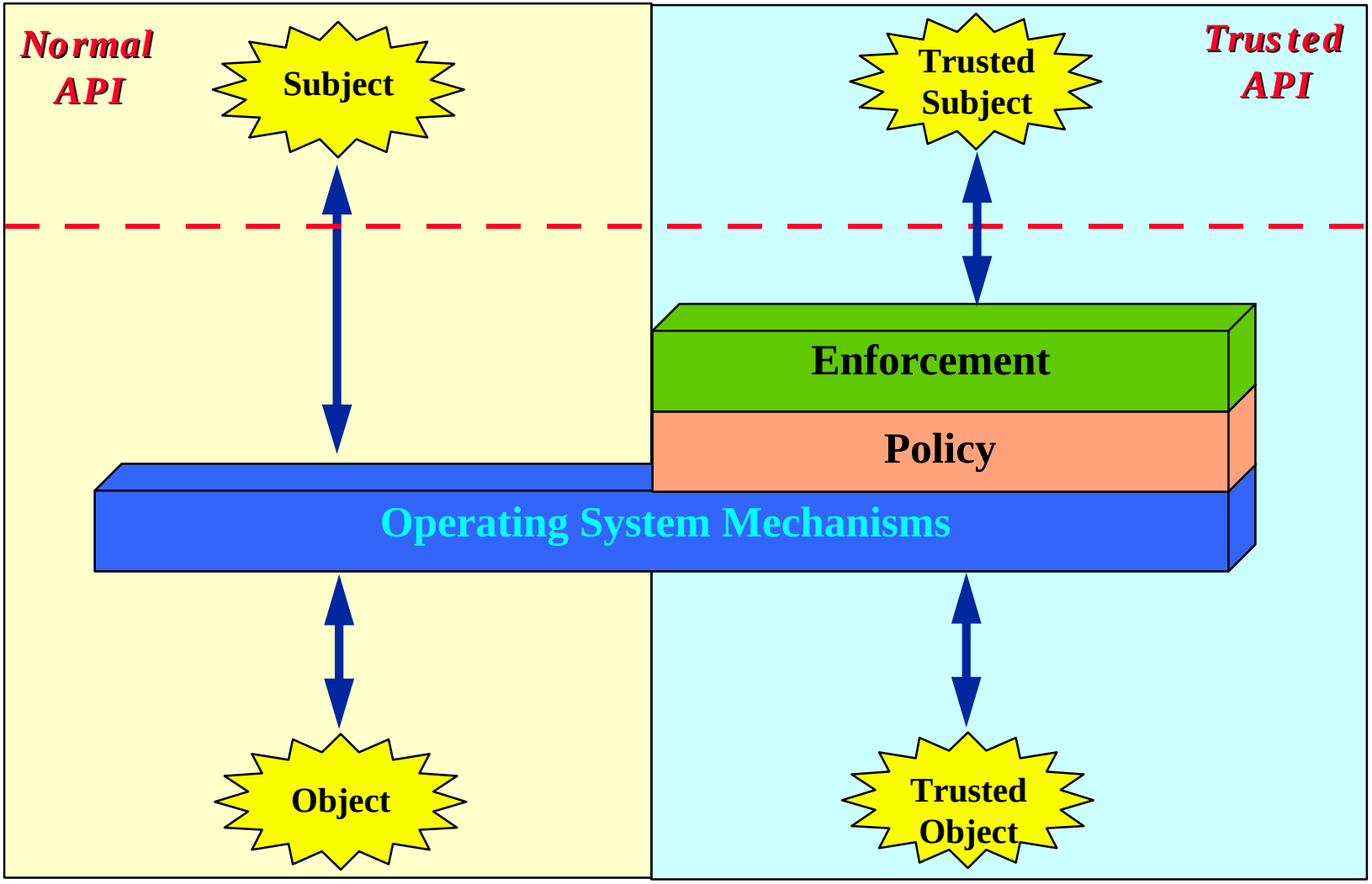
Raytheon

Distributed Security Levels



Raytheon

Dual APIs



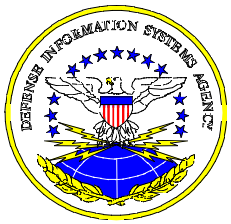
Raytheon

"Security for Real-Timje Military Systems Addendum to the Delta Document" Summary

- Addendum Report is Available from Curtis Royster (DISA).
- 32 Functional Requirements were Identified and Documented.
- Hughes AOS Results
  - Met 28 of the 32 Requirements (88%).
- POSIX Results
  - Met 14 of the 32 Requirements (44%).
- Not all Requirements are Necessary for All User Environments.
  - Dependent on Implementation and Overall Weapon System Structures.

Raytheon

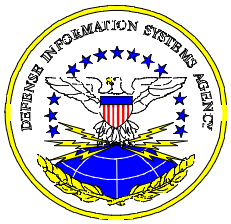
FY98 Summary



- **Security Requirement Document for Standardization**
  - **Identification of RT Embedded Open System Security Requirements is a major accomplishment.**
- **Linwood Sutton (NRAD) has Retired.**
- **There is a Visible Void of Government System Security Advocate Participation at Industry Meetings.**
- **POSIX Security Working Group was Temporarily Dissolved.**
- **Planning for Future Resources and Activities are in Process**
- **New IEEE POSIX PAR Submittal, Security W/G Activity could Participate in Subgroup (Sponsorship Reqd).**

Raytheon

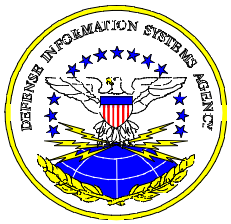
Government POCs



- **Mark Pitarys, (513)255-6548 x3608, pitarysmj@aa.wpafb.af.mil WRDC/AFWAL/AASH WPAFB, Ohio 45433-7003**
- **Curtis Royster, (703)735-3558, roysterc@ncr.disa.mil Defense Information Systems Agency 10701 Parkridge Blvd. Reston, VA 20191-4357**
- **Bill Smith, CISSP, (703)735-3312, smith2b@ncr.disa.mil Defense Information Systems Agency 10701 Parkridge Blvd. Reston, VA 20191-4357**

Raytheon

Executing Agencies



- **Camilo Segura, (310)334-1078, csegura@mail.hac.com**
  Raytheon Systems Company
  M/S: RE/R01/A520
  PO Box 92426
  Los Angeles, California 90009-2426
- **Roberta Gotfried, (310)334-7655, rgotfried@mail.hac.com**
  Raytheon Systems Company
  M/S: RE/R01/A519
  PO Box 92426
  Los Angeles, California 90009-2426
- **Minerva Rodriguez, (310)334-7654,**
  mrodriguez2@mail.hac.com
  Raytheon Systems Company
  M/S: RE/R01/A520
  PO Box 92426
  Los Angeles, California 90009-2426